

LAWYERS



## Davis Wright Tremaine LLP

ANCHORAGE BELLEVUE LOS ANGELES NEW YORK PORTLAND SAN FRANCISCO SEATTLE SHANGHAI WASHINGTON, D.C.

PAUL HUDSON  
DIRECT (202) 973-4275  
paulhudson@dwt.com

SUITE 200  
1919 PENNSYLVANIA AVE NW  
WASHINGTON, DC 20006

TEL (202) 973-4200  
FAX (202) 973-4499  
www.dwt.com

February 27, 2009

### VIA ELECTRONIC FILING

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D. C. 20554

**Re: EB Docket 06-36, Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

Annual § 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of company covered by this certification:

**Adams CATV, Inc. d/b/a Adams Cable Service and Adams Digital  
Phone**

Form 499 Filer ID: **826829**

Name of signatory: **Douglas Adams**

Title of signatory: **President**

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, 47 C.F.R. § 64.2009(e), enclosed for filing in the above-referenced docket is the executed annual CPNI Compliance Certificate of Adams CATV, Inc. ("Company").

Attached to the certificate is a summary of Company's CPNI policies and procedures. Because some of the details included in that document could provide a roadmap for unauthorized persons to attempt to obtain CPNI, Company is filing only a redacted version with the Commission's electronic filing system. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, n.167 (rel. April 2, 2007) ("We recognize carrier concerns

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
February 27, 2009  
Page 2

about providing a roadmap for pretexters with this annual filing, and thus we will allow carriers to submit their certifications confidentially with the Commission.”). The redacted language was previously provided to the Enforcement Bureau in Company’s prior-year filing in this docket, and has not changed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "P. Hudson", written in a cursive style.

Paul B. Hudson  
Counsel for Adams CATV, Inc.

Enclosure

**CERTIFICATE OF COMPLIANCE**

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of company covered by this certification:

**Adams CATV, Inc. d/b/a Adams Cable Service and Adams Digital Phone**


Form 499 Filer ID: 826829

Name of signatory: **Douglas Adams**

Title of signatory: **President**

I, Douglas Adams, certify that I am President and thereby an officer of Adams CATV, Inc. ("Company") and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Commission's rules governing use and disclosure of confidential proprietary network information ("CPNI"), as governed by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, and as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

The Company has not received any customer complaints in the past calendar year concerning unauthorized access to or release of CPNI. Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Company has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission. The Company has established procedures to report any breaches to the FBI and United States Secret Service, and it has emphasized in its employee training of the need for vigilance in identifying and reporting unusual activity in order to enable the company to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.



Douglas Adams

President

Adams CATV, Inc.

Executed February 12, 2009

## **CPNI Compliance Policies of Adams CATV Inc.**

*Effective December 8, 2007*

The following summary describes the policies of Adams CATV Inc. (“Company”) implemented as of December 8, 2007 that are designed to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* CPNI is “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

Because the details of this policy could provide a roadmap for unauthorized persons to attempt to subvert these policies and attempt to obtain CPNI, copies of this policy and related training materials are classified as confidential and may be provided only to Company employees or to parties approved by the Company’s CPNI Compliance Manager, General Manager Wendy Hartman. [REDACTED]

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

Company will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of the Company, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Company does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Although current Company policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee responsible for marketing and the CPNI Compliance Manager. If such use is approved, Company shall modify these policies and conduct additional training as needed to assure compliance with the FCC’s rules.

Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Company receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

## **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Above and beyond the specific FCC requirements, Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Company's existing policies that would strengthen protection of CPNI, they should report such information immediately to Company's CPNI Compliance Manager so that Company may evaluate whether existing policies should be supplemented or changed.

### **A. Online Accounts**

To access an on-line account from which a customer can access their CPNI, customer must enter their Account Number as their Login ID and a password that is established in accordance with the requirements herein.

[REDACTED]

### **B. Inbound Calls to Company Requesting CPNI**

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated. CSRs are trained to verify the caller by requesting the account number, telephone number, name on the account and address.

More stringent protections apply to Call Detail Information (CDI), which includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Even after a caller has been authenticated under the process above, a CSR will not reveal Call Detail Information (CDI) to an inbound caller.

[REDACTED]

If an inbound caller is able to provide to the CSR the telephone number called, when it was called, and, if applicable, the amount charged for the call, exactly as that information appears on the bill, then the CSR is permitted to discuss customer service pertaining to that call and that call only. [REDACTED]

### **C. In-Person Disclosure of CPNI at Company Offices**

Company may disclose a customer's CPNI to an authorized person visiting a Company office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

**D. Notice of Account Changes**

Whenever a password or online account is created or changed, Company will provide a notice to a customer address of record. Whenever a postal or e-mail address of record is created or changed, Company will send a notice to customer's prior address of record notifying them of the change. The foregoing notifications are not required when the customer initiates service, including the selection of an email address or creation of an online account at service initiation.

Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Company if they did not authorize the change.

**E. Safeguard of CPNI Databases and Audit Trail**

[REDACTED]

**III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Company CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

Company's CPNI Compliance Manager is the General Manager Wendy Hartman,  
[REDACTED]

It is Company's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate the Company's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

**A. Identifying a "Breach"**

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a Company employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Company's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Company's CPNI Compliance Manager will determine whether it is appropriate to update Company's CPNI policies or training materials in light of any new information; the FCC's rules require Company on an ongoing basis

## **PUBLIC VERSION**

to “take reasonable measures to discover and protect against activity that is indicative of pretexting.”

### **B. Notification Procedures**

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Company CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Company’s FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC’s Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Company will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure.

If Company receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Company will delay notification to customers or the public upon request of the FBI or USSS.

If the Company Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Company still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

## **IV. RECORD RETENTION**

The Company Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Company maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Company later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission’s recordkeeping requirements.

Company maintains a record of all customer complaints related to their handling of CPNI, and records of the Company’s handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that the Company considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

## **PUBLIC VERSION**

Company will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Company has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Company's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

### **V. TRAINING**

All employees with access to CPNI receive a copy of Company's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Company requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel, and completed initial training prior to December 8, 2007. [REDACTED]